kaspersky BRING ON THE FUTURE

XDR vs. SIEM vs. SOAR

Too many acronyms got your head in a spin? Let's find out what's going on behind these little letters...

Introduction

SIEM, SOAR, MDR, EDR, EPP, XDR... are you feeling bewildered, lost in a jungle of cybersecurity acronyms? It's understandable — that's why we've gone and provided this helpful guide to work out the differences between three of the big ones: SIEM, SOAR, and XDR. What's the story behind these acronyms? How is it that the industry has developed these confusing, overlapping terms? Do they even mean anything distinct, or are they just marketing gimmicks? What are the similarities and differences? Can they complement each other, or are they in competition with each other?

Come, join us on this quest! Let us pick up our machetes of knowledge, hack through the forest of acronyms and jargon, and arrive in an open glade of clear understanding!

SIEM

Security information and event management (SIEM) is a set of tools and services that combine security events management (SEM) and security information management (SIM) in a single platform. SIEM collects, aggregates, analyzes and stores log data from across the IT infrastructure for various use cases, including governance and compliance, and rule-based correlation matching for suspicious activity.

How does SIEM work?

The first SIEM services were developed way back in 2005, with the original purpose of aggregating and storing logs and events from across an organization's IT infrastructure — including endpoints, applications and network devices — for compliance reporting purposes. The SIEM runs correlations on this data set, looking for any patterns or events that might indicate suspicious behavior, and generates an alert for the security operations center (SOC). Security analysts soon saw the possibility of using these alerts not only for compliance and governance purposes, but to more proactively identify and halt the progress of any malicious activity in the ecosystem.

SIEM limitations

The problem was that SIEM services were not designed for the specific purpose of detecting and responding to incidents. This made them a little difficult to work with, for a number of reasons:

- Too many alerts — The huge data set provided by the SIEM has to be manually filtered, processed, and analyzed, which is not convenient for security analysts trying to prevent attacks in a fast-paced threatscape.
- No context — To deal with new, complex, sophisticated attacks, security analysts need a contextualized, coherent picture of the organization's threatscape, rather than the disconnected data streams provided by the SIEM.
- Too passive — Blocking suspicious processes, quarantining files and other response capabilities are not within its remit; it's basically a passive, analytical tool.

Security professionals have attempted to solve these problems by layering additional tools on top of the SIEM, or developing new generations with machine learning and behavioral analytics plugins. But the demand for a tool which gives better quality alerts and facilities faster, automated processes remained.

SOAR

Security Orchestration & Automated Response (SOAR) tools emerged in 2015 to resolve some of the above-mentioned faults in SIEM systems. SOAR platforms ingest data from a variety of sources across the infrastructure, including management systems and threat intelligence platforms, and provide priority analysis. Security teams can then configure multi-stage, cross-solution automated responses to incoming threats, using the SOAR platform's integration of an API-connected ecosystem of security tools.

How does SOAR work?

This time, the name is actually quite helpful! Here's why:

SOAR tools Automate. While often best known for their capacity to automate incident response processes, these tools can actually automate a wide range of workflows, including vulnerability scanning, log analysis, user access management, threat triage and more. They do this using "playbooks" — sets of pre-configured rules triggered by specific events, which tell the system which steps should be taken next in a specific workflow. Most SOAR solutions come with hundreds of ready-to-use playbooks, covering the most common tasks faced by SOC teams. Teams can then configure their own playbooks to automate other, more particular repetitive processes they may have.

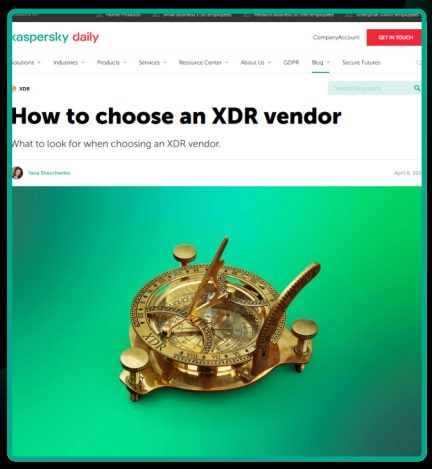
Then, they Orchestrate. While automation refers to the machine-driven execution of individual tasks within a single workflow, orchestration refers to the coordination of multiple disparate tools and processes into a larger workflow, collating all relevant data into a single platform for consolidated, actionable information.

The relationship between SIEM and SOAR

Typically, an SIEM is used in tandem with SOAR tools in something like an assistant-manager relationship: the SIEM collects up all the logs, correlates them to find alerts, and serves this info to the SOAR, which can then take the lead on response actions.

How to choose an XDR vendor?

Many cybersecurity vendors have jumped on the XDR bandwagon with their own solutions. How can you know if you're getting a decent product? Check out our helpful guide: https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



SOAR limitations

All sounds pretty great, right? The thing is that maintaining a well-configured SOAR platform which integrates with partner tools requires the ongoing effort of a highly skilled, mature SOC — a resource which many organizations don't have right now, given the current cybersecurity skills gap.

Without such skilled, vigilant maintenance, SOAR analysts can end up with too many low-priority alerts, false positives, and a generally incoherent data set as a result of all the various, siloed tools feeding into the platform — exactly what they were trying to avoid.

XDR

XDR is an on-premise or cloud-based security solution, which comes under broadly two categories: native and hybrid. Native XDR is a unified suite of tools from a single vendor, while Hybrid XDR integrates other third-party solutions in your ecosystem. The term "XDR" was first used in 2018, with the "X" standing for "eXtended": XDR 'extends' beyond traditional endpoint detection, response and protection tools (EDR and EPP) by collecting and correlating data from multiple security layers, including email, cloud and network, to provide comprehensive protection over the entire IT infrastructure.

So, it's a single platform that coordinates a range of tools, and uses machine learning and automation to help security teams protect the entire security ecosystem... sounds a bit similar to SOAR, no? But there are some fundamental differences. Let's take a look...

XDR vs. SOAR: What's the difference?

1. XDR solutions are anchored in endpoint data and optimization — this means that incident detection and response is a central design feature, giving them advanced analysis capabilities that SOAR tools typically don't have. XDR tools are masters at detecting unknown and zero-day threats, leveraging powerful artificial intelligence, machine learning algorithms and threat intelligence to protect an organization beyond its boundaries. On the other hand, SOAR tools can offer a much wider variety of use cases, since they can orchestrate and automate any processes across the infrastructure — not just incident response.
2. XDR can be considered as something like SOAR-lite — a streamlined interface that offers one-click automated responses to incoming threats and alerts. This can be much more convenient for an organization that does not have the resources to maintain the complexity of a well-configured SOAR platform.
3. XDR enables smooth cross-product integration — whether across a single vendor's stack of tools, or third-party products as well, XDR excels at seamless interoperability. SOAR tools often face a struggle in trying to integrate all the disparate, siloed tools in their stack; XDR breaks down these silos for efficient, all-in-one threat response.

So will XDR replace SIEM and SOAR?

The jury is still out on this one, since XDR is relatively new technology which is being continuously developed. Currently, most experts recommend an integrated approach, since each solution offers advantages that complement the others:

- SIEM — the SIEM has use cases outside of threat detection, such as log management, compliance, and analyzing non-threat related data.
- SOAR — the great customizability of SOAR playbooks is useful for orchestrating and automating processes across the organizations infrastructure.
- XDR — when it comes to detecting and responding to threats, the advanced analytics of an XDR solution offer enhanced protection which is second to none.

Looking for a tried and tested, adaptable solution for your experts?
Kaspersky Expert Security, XDR based on a cloud-native EDR solution, provides your organization with enhanced visibility and functionality for AI-based detection and auto response logic across all endpoints and the network, facilitating a wide range of automated incident response scenarios. The platform's built-in advanced technology for detection and analysis is complemented by world-leading threat intelligence. Kaspersky XDR's unified architecture provides centralized management from a single web console. To learn more please visit go.kaspersky.com/expert.

www.kaspersky.com